Business Impact Analysis Sistem Dan Jaringan Komputer Menggunakan Metode Network Security Assessment

I Gede Putu Krisna Juliharta
Program Studi Manajemen Sistem Informasi
Pogram Pascasarjana, Universitas Udayana
Email :krisna@stikom-bali.ac.id

Abstrak

Pemerintah Kota Denpasar merupakan institusi atau organisasi yang memberikan pelayan terhadap masyarakat Denpasar dan merupakan perpanjangan dari Pemerintah pusat. Dalam proses pelayanan Pemerintah Kota Denpasar menggunakan jaringan dan internet. Dengan penerapan jaringan, pelayanan bisa dilakukan dengan sistem pelayanan "satu atap", koordinasi antara instansi juga dapat dilakukan dengan cepat, yang berdampak positif terhadap proses pelayanan kepada masyarakat. Hingga saat ini pengelolaan teknologi informasi (TI) di Pemerintah Kota Denpasar belum terkelola dengan baik, salah satunya analisa Business Impact Analysis Belum pernah dilakukan. Agar penggunaan teknologi di Pemerintah Kota Denpasar dapat berjalan secara efektif, Pemerintah Kota Denpasar perlu melakukan business impact analysis terhadap penerapan jaringan komputer dan teknologi informasi yang telah digunakan. Salah satu cara adalah dengan melakukan penilaian terhadap jaringan komputer Pemerintah Kota Denpasar menggunakan metode network security assessment. Proses tersebut meliputi network reconnaissance, bulk network scanning and probing, dan investigasi vulnerability.Dari hasil network security assessment tersebut proses dilanjutkan ke tahapan business impact analysis. Hasil dari proses business impact analysis, didapatkan kesimpulan bahwa dalam penerapan jaringan komputer Pemerintah Kota Denpasar menunjukkan sistem yang ada di dalam jaringan Pemerintah Kota Denpasar memiliki vulnerability dengan rata rata sebanyak 15, 8 vulnerability dan dari 6 server yang dilakukan Business Impact Analysis terdapat 4 server memiliki peringkat resiko critical atau high, yaitu server Email, Eproc, SIPKD, dan Simpeg. Untuk saran penelitian selanjutnya business impact analysis dapat melakukan perhitungan kuantitatif, dan hasil dari business impact analysis dapat dijadikan acuan untuk membangun disaster recovery planning.

Kata kunci: *Teknologi Informasi, sistem dan jaringan komputer,, Network Security Assessment, Business Impact Analysis*

Abstract

Denpasar City Government is an institution or organisation that gives services to the society of Denpasar and is an extention of the Main Government of Indonesia. In their service process, the Denpasar City Government use network and internet. By applying the network, services can be done by "one roof" service system, coordination between instances can also be done quickly which has a positive impact into the service process to the society. Until now the Information Technology (IT) management in Denpasar City Government has not been managed well, one of them is that the business impact analysis which has never been done before. If the Denpasar City Government wants the use of technology runs effectively, then the government needs to do a business impact analysis to the application of computer network and information technology that have been used. One of the ways to do it is by giving an assessment to the computer network in Denpasar City Government by using network security assessment method. This process includes network reconnaissance, bulk network scanning and probing, and vulnerability investigation. Based on that network security assessment, the process is then continued to the business impact analysis. From the results of the business impact analysis,it is acquired a conclusion that in applying their network computer, Denpasar City Government have vulnerability inside their network with approximitely 15,8 vulnerabilities and from 6 servers that are checked with business impact analysis, there are 4 servers which are rated critical or high risk, they are the email, Eproc, SIPKD,and Simpeg. Suggestion for the next research is that business impact analysis can do quantitative calculation, and the results from the business impact analysis can be used as reference to build a disaster recovery planning.

Keywords: *Information Technology, Computer and Network System, Network Security Assessment, Business Impact Analysis*

1. Pendahuluan

Langkah besar dalam mengukur tingkat resiko adalah menentukan dampak buruk yang dihasilkan dari analisa kelemahan.Tujuan dari *BusinessImpact Analysis* (BIA) adalah memprioritaskan tingkat dampak yang terkait dengan aset informasi organisasi berdasarkan penilaian kualitatif atau kuantitatif dari kepekaan dan kekritisan aset.Beberapa dampak yang nyata dapat diukur secara kuantitatif terhadap kehilangan pendapatan, biaya perbaikan sistem, atau tingkat usaha yang dibutuhkan untuk memperbaiki masalah yang disebabkan oleh ancaman yang berjalan. Dampak lainnya (misalnya, hilangnya kepercayaan masyarakat, kehilangan kredibilitas, kerusakan terhadap kepentingan organisasi) tidak dapat diukur dalam satuan khusus, namun dapat dikualifikasikan atau digambarkan dalam dengan parameter *High* (tinggi), *Medium* (sedang) , dan *Low* (rendah).

Salah satu cara untuk mengukur *Business Impact Analysis* dari penggunaan sistem dan jaringan komputer di suatu organisasi adalah dengan cara melakukan *Network*Security *Asessment* (Penilaian Keamanan Jaringan) pada jaringan yang digunakan oleh organisasi tersebut.*Network Security Assessment*merupakan gabungan penilaian otomatisasi, manual vulnerability testing, dan kualifikasi jaringan. Penilaian keamanan jaringan merupakan bagian integral dari siklus hidup keamanan, laporan dari hasil penilaian biasanya berupa tulisan tangan yang akurat dan ringkas, dengan tujuan memberikan nasihat praktis yang dapat meningkatkan keamanan perusahaan.

Pemerintah Kota Denpasar merupakan sebuah institusi yang menggunakan Sistem dan Jaringan Komputer dalam proses pelayananya terhadap masyarakat. Maka dari itu penelitian yang akan dilakukan akan mengukur *Business Impact Analysis* dari jaringan Pemerintah Kota Denpasar dengan menggunakan metode *Network Security Assessment*.

Berdasarkan pendahuluan tersebut, dibuatlah rumusan masalah dari penelitian yang akan dilakukan. Rumusan masalah dari penelitian ini adalah :

1. Bagaimana menguji jaringan yang sudah ada dengan *Network Security Assessment*?
2. Bagaimana membangun *Business Impact Analysis*berdasarkan hasil dari *Network Security Assessment*?

Tujuan dari penelitian ini adalah :

1. Memberikan kontribusi bagi pengelolaan jaringan di pemerintah kota Denpasar.
2. Memberikan rekomendasi tentang dampak yang dihadapi dari penerapan sistem dan jaringan di Pemerintah Kota Denpasar.

Tanpa batasan masalah penelitian yang dilakukan sangatlah luas ruang lingkupnya, maka dari itu dirasa perlu untuk membatasi sejauh mana penelitian ini akan dilakukan. Batasan masalah meliputi :

1. *Business Impact Analysis* yang berdasarkan hasil dari*Network Security Assessment*
2. *Network Security Assessment*dilakukan pada jaringan Satuan Kerja Perangkat daerah (SKPD) Pemerintah Kota Denpasar yang dikelola oleh Dinas Komunikasi dan Informatika Kota Denpasar.
3. *Network security assesment* yang dilakukan meliputi :*Network reconnaissance, Bulk network scanning and probing,* Investigasi *vulnerabilities*.

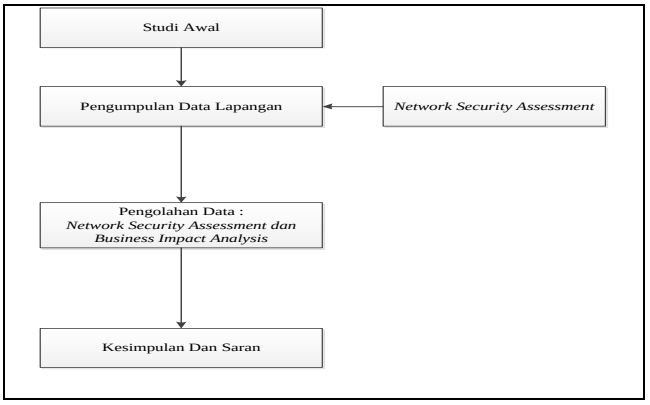
2. Metode Penelitian

2.1. Tempat dan Waktu Penelitian.

Tempat dan waktu penelitian dilakukan di Pemerintah Kota Denpasar, diumulai dari bulan Maret 2012 hingga Juni 2012.

2.2. Perancangan Penelitian

Dalam melakukan penelitian ini, penulis melakukan langkah-langkah penelitian yang dapat digambarkanpada gambar 1 :



Gambar 1. Langkah Penelitian

a. Studi awal
Dalam melakukan studi awal, penulis melakukan : pencarian materi, perancangan teknik-teknik*NetworkSecurity Assessment* apa yang akan digunakan, mempelajari jaringan komputer yang telah berjalan.

b. Pengumpulan data lapangan
Pada tahapan ini, penulis melakukan pengumpulan data yang diperoleh dengan cara melakukan observasi, wawancara, dan melakukan proses *Network Security Assessment*

c. Pengolahan data
Pada tahapan ini, penulis melakukan pengolahan data dari hasil observasi, wawancara, dan *Network Security Assesment*, dan *Business Impact Analysis*

d. Kesimpulan dan Saran.
Pada tahap akhir penulis membuat kesimpulan dan saran dari semua proses penelitian yang dilakukan

2.3. Instrumen Penelitian

Alat penelitian yang akan digunakan dalam penelitian dibagi dalam dua bagian utama yaitu:

a. Perangkat Lunak
Perangkat lunak yang digunakan dalam perancangan sistem terdiri dari dua bagian yaitu :
1. SistemOperasiyaitu,Linux dan Windows
2. *Network Security Tools*

Menggunakan beberapa *tools* yang disediakan dinternet, *tools* yang digunakan bersifat *freeware*.

Tabel 1*Tools Network Security Assessment*

TOOLS	**FUNGSI**
Ping (Fping, Gping)	*Network enumeration* dan identifikasi *ip address* yang aktif
Nessus	○ *Network security scanner dan vulnerability* ○ *Port scanner dan penetration testing TCP, UDP, SNMP, URL* ○ *Network protocol analyzer*
Traceroute	*Menganalisa jalur paket data mengalir*

b. Perangkat Keras
Perangkat keras yang digunakan dalam penelitian adalah:
1. Komputer dengan spesifikasi
   - Processor Intel Centrino Duo 1,8GHz
   - 2 GB RAM
   - Hardisk 160 GB
   - VGA 256 MB

HDD External 500 GB

3. Hasil dan Analisis

3.1. *Network Security Assessment*

Network security assessment jaringan komputer Pemerintah Kota Denpasar diidentifikasi selama sebulan dimulai dari tanggal 21 Mei sampai 13 juni 2012

a. *Network Reconnaissance*

Untuk proses *network Reconnaissance* ada beberapa tools yang digunakan. Semuanya bersifat web-base*yaitu* :http://domainwhitepages.com, http://magic-info.net. Untuk hasilnya dapat dilihat pada tabel 2 sampai tabel 3

Tabel 2 Hasil domainwhitepages.com

	KETERANGAN
Nama	Bali Medianet
Alamat	Jl. Tukad Batanghari No. 88 Panjer Denpasar Bali
Contact email	fpranadi@balimedianet.com
Email teknis	noc@balimedianet.com
Email spam	abuse@balimedianet.com
Telp	0361 7421099

Tabel 3 Hasil Magic-info.net

NO	**IP ADDRESS**	**NAMA MESIN**	**TIPE**
1	202.169.237.58	jempiring.denpasarkota.go.id	*Public*
2	111.92.160.8	lawar.denpasarkota.go.id	*Public*
3	111.92.160.4	qmail.denpasarkota.go.id	*Public*
4	202.169.237.66	eproc.denpasarkota.go.id	*Public*
5	202.169.237.74	gis.denpasarkota.go.id	*Public*
6	192.168.152.2	simpeg.denpasarkota.go.id	Private

Sedangkan dengan pengamatan secara langsung terdapat satu lagi server yang bersifat *private* yaitu server Sistem Informasi Pengelolaan Keuangan Daerah (SIPKD), sehingga total server yang dimiliki oleh Pemerintah Kota Denpasar Sebanyak 7 buah

Tabel 4 Hasil *Network Reconnaissance*

NO	**IP ADDRESS**	**NAMA MESIN**	**TIPE**	**FUNGSI**
1	202.169.237.58	jempiring.denpasarkota.go.id	*Public*	Web server
2	111.92.160.8	lawar.denpasarkota.go.id	*Public*	Web dan DNS server
3	111.92.160.4	qmail.denpasarkota.go.id	*Public*	Mail server
4	202.169.237.66	eproc.denpasarkota.go.id	*Public*	Web Server
5	202.169.237.74	gis.denpasarkota.go.id	*Public*	Web server
6	192.168.152.2	simpeg.denpasarkota.go.id	*Private*	Web server
7	192.168.133.93	SIPKD	*Private*	Web Server

b. *Bulk network scanning and probing*

Tahapan *bulk network scanning and probing* dilakukan selama satu bulan dari tanggal 21 mei 2012 sampai 13 juni 2012 dengan menggunakan 2 *tools* karena tujuannya hanya untuk mengetahui sistem tersebut menyala atau tidak, *tools* yang digunakan untuk melakukan proses ini adalah ping dan traceroute/tracert dengan hasil ditujunjukkan pada tabel 5 :

Tabel 5 Proses *Ping*

NO	**IP ADDRESS**	**NAMA MESIN**	***PING* STATUS**
1	202.169.237.58	jempiring.denpasarkota.go.id	*Reply*
2	111.92.160.8	lawar.denpasarkota.go.id	*Request Time Out*
3	111.92.160.4	qmail.denpasarkota.go.id	*Request Time Out*
4	202.169.237.66	eproc.denpasarkota.go.id	*Request Time Out*
5	202.169.237.74	gis.denpasarkota.go.id	*Request Time Out*
6	192.168.152.2	simpeg.denpasarkota.go.id	*Reply*
7	192.168.133.93	SIPKD	*Reply*

Proses ping, mesin jempiring, simpeg, dan SIPKD memberikan status *reply* yang berarti sudah dipastikan bahwa server tersebut menyala. Sedangkan untuk jawaban *request time out* perlu dibuktikan lagi dengan melakukan proses *traceroute* untuk memastikan apa memang benar server dengan *IP Address* tertentu memang mati atau tidak ada (tabel 6).

Tabel 6 Proses *Traceroute*

NO	IP ADRESS	HASIL *TRACEROUTE*	
1	202.169.237.58	Lokasi	Indonesia
		Firewall	*Ping* diizinkan
		Route length	9 hops
		Loss	0 %
		Status	Up
2	111.92.160.8	Lokasi	Indonesia
		Firewall	*Ping* tidak diizinkan
		Route length	9 hops
		Loss	100%
		Status	UP
3	111.92.160.4	Lokasi	Indonesia
		Firewall	*Ping* tidak diizinkan
		Route length	9 hops
		Loss	100 %
		Status	Up
4	202.169.237.66	Lokasi	Indonesia
		Firewall	*Ping* tidak diizinkan
		Route length	9 hops
		Analysis	waktu respon rata rata 63 ms
		Status	Up
5	202.169.237.74	Lokasi	Indonesia
		Firewall	*Ping* tidak diizinkan
		Route length	9 hops
		Analysis	waktu respon rata rata 63 ms
		Status	Down
6	192.168.152.2	Lokasi	Indonesia
		Firewall	*Ping* diizinkan
		Route length	3 hops
		Analysis	0 %
		Status	Up
7	192.168.133.93	Lokasi	Indonesia
		Firewall	*Ping* diizinkan
		Route length	3 hops
		Analysis	0 %
		Status	Up

Hasil proses *traceroute* dan *ping* pada tabel 4.6 sampai tabel 4.7 didapatkan beberapa fakta diataranya, server jempiring, simpeg, dan SIPKD untuk *ping* statusnya *reply* dan dalam *traceroute* juga *Up* (menyala). Hal ini dapat dipastikan bahwa ketiga server hidup dan memberikan layanan.Server lawar, qmail, dan eproc untuk statusnya adalah *request time out* dan dalam *tracerouteUp* (menyala). Hal ini dapat dipastikan bahwa ketiga server menyala namun ketiga server memblokir layanan *ping*.Server sig status *ping* adalah *request time out* dan *traceroute* adalah *down* (mati), maka dapat dipastikan bahwa server sig tidak aktif. Oleh karena untuk proses selanjutnya yaitu melakukan investigasi *vulnerabilities*dan *Business Impact Analysis* server sig tidak dimasukkan dalam proses investigasi.

c. Investigasi *Vulnerabilities*

Proses akhir dari *Network Security Assessment*adalah melakukan investigasi *vulnerabilities*. Perangkat yang diinvetigasi adalah perangkat hasil dari proses sebelumnya.

Tabel 7. Server Yang Dilakukan *Investigasi Vulnerability*

NO	IP ADDRESS	NAMA MESIN
1	202.169.237.58	Jempiring.denpasarkota.go.id
2	111.92.160.8	Lawar.denpasarkota.go.id
3	111.92.160.4	Qmail.denpasarkota.go.id
4	202.169.237.66	Server E-procuremen
5	192.168.133.93	Server Sistem Informasi pengelolaan keuangan daerah
6	192.168.152.2	Server Kepegawaian

Dari tabel 7 diatas dapat digambarkan satu persatu bagaimana kerentanan dari setiap mesin atau server. Kerentanan atau *vulnerability* setiap server didapatkan dengan cara melakukuan

scanning ke perangkat tersebut menggunakan*tools* nessus.Hasil dari *vulnerability assessment* dapat dilihat di tabel8 sampai tabel 14.

Tabel 8. Kerentanan Server Jempiring.denpasarkota.go.id

NO	*VULNERABILITY*	JENIS KERENTANAN
1	*Web Server info.php / phpinfo.php Detection*	*CGI abuses*
2	*PHP expose_php Information Disclosure*	*Web servers*
3	*SQL Dump Files Disclosed via Web Server*	*CGI abuses*
4	*Apache HTTP Server httpOnly Cookie Information Disclosure*	*Web servers*
5	*Web Server Uses Plain Text Authentication Forms*	*Web servers*

Tabel 9. Kerentanan Server lawar.denpasarkota.go.id

NO	*VULNERABILITY*	JENIS KERENTANAN
1	*SSL Certificate Cannot Be Trusted*	*General*
2	*SSL Self-Signed Certificate*	*General*
3	*Anonymous FTP Enabled*	*FTP*
4	*Web Server info.php / phpinfo.php Detection*	*CGI Abuse*
5	*SSL Certificate Expiry*	*General*
6	*SSL Certificate with Wrong Hostname*	*General*
7	*PHP expose_php Information Disclosure*	*Web server*
8	*HTTP TRACE / TRACK Methods Allowed*	*Web server*
9	*SSL Medium Strength Cipher Suites Supported*	*General*
10	*Apache HTTP Server httpOnly Cookie Information Disclosure*	*Web server*
11	*FTP Supports Clear Text Authentication*	*FTP*
12	*SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection*	*General*
13	*SSL / TLS Renegotiation DoS*	*General*

Tabel 10. Kerentanan Server *email*

NO	*VULNERABILITY*	JENIS KERENTANAN
1	*MTA Open Mail Relaying Allowed (thorough test)*	*SMTP problems*
2	*Apache HTTP Server Byte Range DoS*	*Web server*
3	*Asterisk Skinny Channel Driver (chan_skinny) get_input Function Remote Overflow*	*Gain a Shell remotely*
4	*Default Password (changeme) for SHOUTcast Server Service Port*	*CGI abuses*
5	*SSL Certificate Cannot Be Trusted*	*General*
6	*SSL Self-Signed Certificate*	*General*
7	*SSL Certificate Expiry*	*General*
8	*SSL Version 2 (v2) Protocol Detection*	*Service Detection*
9	*PHP expose_php Information Disclosure*	*Web server*
10	*HTTP TRACE / TRACK Methods Allowed*	*Web server*
11	*SSL Weak Cipher Suites Supported*	*General*
12	*SSL Medium Strength Cipher Suites Supported*	*General*
13	*phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)*	*CGI abuses : XSS*
14	*Apache HTTP Server httpOnly Cookie Information Disclosure*	*Web servers*
15	*IMAP Service STARTTLS Plaintext Command Injection*	*Misc.*
16	*SMTP Service STARTTLS Plaintext Command Injection*	*SMTP problems*
17	*Web Server Uses Plain Text Authentication Forms*	*Web server*
18	*SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection*	*General*
19	*SSL / TLS Renegotiation DoS*	*General*
20	*SMTP Service Cleartext Login Permitted*	*SMTP problems*

Tabel 11. Kerentanan Server Eproc

NO	*VULNERABILITY*	JENIS KERENTANAN
1	*Apache 2.2 < 2.2.15 Multiple Vulnerabilities*	*Web Servers*
2	*Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow*	*Web Servers*
3	*Apache HTTP Server Byte Range DoS*	*Web Servers*
4	*SNMP Agent Default Community Name (public)*	*SNMP*
5	*Apache 2.2 < 2.2.14 Multiple Vulnerabilities*	*Web Servers*
6	*Apache 2.x < 2.2.12 Multiple Vulnerabilities*	*Web Servers*
7	*SSL Certificate Cannot Be Trusted*	*General*
8	*SSL Self-Signed Certificate*	*General*

Tabel 12.Lanjutan Kerentanan Server Eproc

NO	*VULNERABILITY*	JENIS KERENTANAN
9	*SSL Certificate Expiry*	*General*
10	*SSL Certificate with Wrong Hostname*	*General*
11	*Apache 2.2 < 2.2.16 Multiple Vulnerabilities*	*Web Servers*
12	*Apache 2.2 < 2.2.17 Multiple Vulnerabilities*	*Web Servers*
13	*Apache 2.2 < 2.2.22 Multiple Vulnerabilities*	*Web Servers*
14	*HTTP TRACE / TRACK Methods Allowed*	*Web Servers*
15	*Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)*	*Web Servers*
16	*SSL Medium Strength Cipher Suites Supported*	*General*
17	*Apache 2.2 < 2.2.18 APR apr_fnmatch DoS*	*Web Servers*
18	*Apache 2.2 < 2.2.21 mod_proxy_ajp DoS*	*Web Servers*
19	*Apache HTTP Server httpOnly Cookie Information Disclosure*	*Web Servers*
20	*SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection*	*General*
21	*SSL / TLS Renegotiation DoS*	*General*

Tabel 13. Kerentanan Server SIPKD

NO	*VULNERABILITY*	JENIS KERENTANAN
1	*35362 MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution*	*Windows*
2	*Conficker Worm Detection (uncredentialed check)*	*Backdoors*
3	*MS09-039: Vulnerabilities in WINS Could Allow Remote Code Execution*	*Windows*
4	*HP* Sistem *Management Homepage < 6.3 Multiple Vulnerabilities*	*Web servers*
5	*Multiple Vendor DNS Query ID Field Prediction Cache Poisoning*	*DNS*
6	*MS11-035: Vulnerability in WINS Could Allow Remote Code Execution*	*Windows*
7	*MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution*	*Windows*
8	*HP* Sistem *Management Homepage < 6.2 Multiple Vulnerabilities*	*Web servers*
9	*JBoss JMX Console Unrestricted Access*	*CGI abuses*
10	*SSL Certificate Cannot Be Trusted*	*General*
11	*SSL Self-Signed Certificate*	*General*
12	*Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness*	*Windows*
13	*Chargen UDP Service Remote DoS*	*Denial Of Service*
14	*Multiple Server Crafted Request WEB-INF Directory Information Disclosure*	*CGI abuses*
15	*DNS Server Cache Snooping Remote Information Disclosure*	*DNS*
16	*SSL Certificate Expiry*	*General*
17	*Microsoft Windows SMB NULL Session Authentication*	*Windows*
18	*SMB Signing Disabled*	*Misc.*
19	*SSL Weak Cipher Suites Supported*	*General*
20	*SSL Medium Strength Cipher Suites Supported*	*General*
21	*Terminal Services Encryption Level is Medium or Low*	*Misc.*
22	*SSL Certificate Signed using Weak Hashing Algorithm*	*General*
23	*Terminal Services Encryption Level is not FIPS-140 Compliant*	*Misc.*
24	*SSL / TLS Renegotiation DoS*	*General*

Tabel 14. Kerentanan server SIMPEG

NO	*VULNERABILITY*	JENIS KERENTANAN
1	*MS03-026: Microsoft RPC Interface Buffer Overrun*	*Windows*
2	*MS03-039: Microsoft RPC Interface Buffer Overrun*	*Windows*
3	*MS04-007: ASN.1 Vulnerability Could Allow Code Execution*	*Windows*
4	*MS04-011: Security Update for Microsoft Windows*	*Windows*
5	*MS05-027: Vulnerability in SMB Could Allow Remote Code Execution*	*Windows*
6	*MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution*	*Windows*
7	*MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution*	*Windows*
8	*MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution*	*Windows*
9	*MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution*	*Windows*
10	*Microsoft Windows SMB NULL Session Authentication*	*Windows*
11	*SMB Signing Disabled*	*Misc.*

Investigasi *vulnerability* merupakan tahap akhir dari *Network Security Assessment*. Tabel 8 sampai tabel 14 merupakan hasil investigasi *vulnerability*, dengan hasil *vulnerability*, server jempiring memiliki 5 *vulnerability*, server lawar sebanyak 13 *vulnerability*, server *email* 20 *vulnerability*, server eproc sebanyak 21 *vulnerability*, server SIPKD sebanyak 24 *vulnerability*, dan server Simpeg sebanyak 11 *vulnerability*. Dalam keamanan jaringan adanya *vulnerability* pada sistem menimbulkan resiko dan konsekuensi yang sangat besar terhadap *integrity*, *availability*, dan *confidentiality* dari keamanan jaringan dan sistem informasi.

3.2. *Business Impact Analysis* Server Kota Denpasar

Hasil investigasi vulnerability yang didapatkan pada proses *Network Security Assessment*proses selanjutnya adalah menghitung *business impact analysis* (BIA). Proses BIA menggunakanstandar penilaian CVSS versi 2 dengan skala yang disebutkan pada tabel 15.

Tabel 15. penghitungan Level

ATURAN	*LEVEL*
0 <*score*< 4	*Low*
4 ≤ *score*< 7	*Medium*
7 ≤ *score*<10	*High*
10	*Critical*

Untuk *Business Impact Analisis* dari server Kota Denpasardapat dilihat pada tabel 16. sampai tabel 24. :

Tabel 16. *Business Impact Analysis* Server Jempiring

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
1	*Web Server info.php / phpinfo.php Detection*	1.0	0.71	0.740	0.275	0.0	0.0	2.9	10	5	*Medium*
2	*PHP expose_php Information Disclosure*	1.0	0.71	0.740	0.275	0.0	0.0	2.9	10	5	*Medium*
3	*SQL Dump Files Disclosed via Web Server*	1.0	0.71	0.740	0.275	0.0	0.0	2.9	10	5	*Medium*
4	*Apache HTTP Server httpOnly Cookie Information Disclosure*	1.0	0.61	0.740	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
5	*Web Server Uses Plain Text Authentication Forms*	1.0	0.35	0.740	0.275	0.0	0.0	2.9	4.9	2.6	*Low*

Tabel 17. *Business Impact Analysis* Server Lawar

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
1	*SSL Certificate Cannot Be Trusted*	1.0	0.71	0.714	0.275	0.275	0.0	4.9	10	6.4	*Medium*
2	*SSL Self-Signed Certificate*	1.0	0.71	0.714	0.275	0.275	0.0	4.9	10	6.4	*Medium*
3	*Anonymous FTP Enabled*	1.0	0.71	0.714	0.275	0.0	0.0	2.9	10	5	*Medium*
4	*Web Server info.php / phpinfo.php Detection*	1.0	0.71	0.714	0.275	0.0	0.0	2.9	10	5	*Medium*
5	*SSL Certificate Expiry*	1.0	0.71	0.714	0.0	0.275	0.0	2.9	10	5	*Medium*
6	*SSL Certificate with Wrong Hostname*	1.0	0.71	0.714	0.0	0.275	0.0	2.9	10	5	*Medium*
7	*PHP expose_php Information Disclosure*	1.0	0.71	0.714	0.275	0.0	0.0	2.9	10	5	*Medium*
8	*HTTP TRACE / TRACK Methods Allowed*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
9	*SSL Medium Strength Cipher Suites Supported*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
10	*Apache HTTP Server httpOnly Cookie Information Disclosure*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
11	*FTP Supports Clear Text Authentication*	1.0	0.35	0.704	0.275	0.0	0.0	2.9	4.9	2.6	*Low*
12	*SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection*	1.0	0.35	0.704	0.0	0.275	0.0	2.9	4.9	2.6	*Low*
13	*SSL / TLS Renegotiation DoS*	1.0	0.35	0.704	0.0	0.0	0.275	2.9	4.9	2.6	*Low*

Tabel 18. *Business Impact Analysis* Server Email

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
1	*MTA Open Mail Relaying Allowed (thorough test)*	1.0	0.71	0.704	0.0	0.0	0.660	6.9	10	7.8	*High*
2	*Apache HTTP Server Byte Range DoS*	1.0	0.71	0.704	0.0	0.0	0.660	6.9	10	7.8	*High*
3	*Asterisk Skinny Channel Driver (chan_skinny) get_input Function Remote Overflow*	1.0	0.71	0.704	0.275	0.275	0.275	6.4	10	7.5	*High*
4	*Default Password (changeme) for SHOUTcast Server Service Port*	1.0	0.71	0.704	0.275	0.275	0.275	6.4	10	7.5	*High*
5	*SSL Certificate Cannot Be Trusted*	1.0	0.71	0.704	0.275	0.275	0.0	4.9	10	6.4	*Medium*
6	*SSL Self-Signed Certificate*	1.0	0.71	0.704	0.275	0.275	0.0	4.9	10	6.4	*Medium*
7	*SSL Certificate Expiry*	1.0	0.71	0.704	0.0	0.275	0.0	2.9	10	5	*Medium*
8	*SSL Version 2 (v2) Protocol Detection*	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*

9	*PHP expose_php Information Disclosure*	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*
10	*HTTP TRACE / TRACK Methods Allowed*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
11	*SSL Weak Cipher Suites Supported*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
12	*SSL Medium Strength Cipher Suites Supported*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
13	*phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)*	1.0	0.61	0.704	0.0	0.275	0.0	2.9	8.6	4.3	*Medium*
14	*Apache HTTP Server httpOnly Cookie Information Disclosure*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
15	*IMAP Service STARTTLS Plaintext Command Injection*	1.0	0.35	0.704	0.275	0.275	0.0	4.9	4.9	4	*Medium*

Tabel 19. Lanjutan *Business Impact Analysis* Server Email

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
16	*SMTP Service STARTTLS Plaintext Command Injection*	1.0	0.35	0.704	0.275	0.275	0.0	4.9	4.9	4	*Medium*
17	*Web Server Uses Plain Text Authentication Forms*	1.0	0.35	0.704	0.275	0.0	0.0	2.9	4.9	2.6	*Low*
18	*SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection*	1.0	0.35	0.704	0.0	0.275	0.0	2.9	4.9	2.6	*Low*
19	*SSL / TLS Renegotiation DoS*	1.0	0.35	0.704	0.0	0.0	0.275	2.9	4.9	2.6	*Low*
20	*SMTP Service Cleartext Login Permitted*	1.0	0.35	0.704	0.0	0.0	0.275	2.9	4.9	2.6	*Low*

Tabel 20. *Business Impact Analysis* Server Eproc

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
1	*Apache 2.2 < 2.2.15 Multiple Vulnerabilities*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
2	*Apache 2.2 < 2.2.13 APR apr_palloc Heap Overflow*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
3	*Apache HTTP Server Byte Range DoS*	1.0	0.71	0.74	0.0	0.0	0.660	6.9	10	7.8	*High*
4	*SNMP Agent Default Community Name (public)*	1.0	0.71	0.74	0.275	0.275	0.275	6.4	10	7.5	*High*
5	*Apache 2.2 < 2.2.14 Multiple Vulnerabilities*	1.0	0.71	0.74	0.275	0.275	0.275	6.4	10	7.5	*High*
6	*Apache 2.x < 2.2.12 Multiple Vulnerabilities*	1.0	0.71	0.74	0.275	0.0	0.275	4.9	10	6.4	*Medium*
7	*SSL Certificate Cannot Be Trusted*	1.0	0.71	0.74	0.275	0.275	0.0	4.9	10	6.4	*Medium*
8	*SSL Self-Signed Certificate*	1.0	0.71	0.74	0.275	0.275	0.0	4.9	10	6.4	*Medium*
9	*SSL Certificate Expiry*	1.0	0.71	0.74	0.0	0.275	0.0	2.9	10	5	*Medium*
10	*SSL Certificate with Wrong Hostname*	1.0	0.71	0.74	0.0	0.275	0.0	2.9	10	5	*Medium*
11	*Apache 2.2 < 2.2.16 Multiple Vulnerabilities*	1.0	0.71	0.74	0.275	0.0	0.0	2.9	10	5	*Medium*
12	*Apache 2.2 < 2.2.17 Multiple Vulnerabilities*	1.0	0.71	0.74	0.0	0.0	0.275	2.9	10	5	*Medium*
13	*Apache 2.2 < 2.2.22 Multiple Vulnerabilities*	1.0	0.71	0.74	0.275	0.0	0.0	2.9	10	5	*Medium*
14	*HTTP TRACE / TRACK Methods Allowed*	1.0	0.61	0.74	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
15	*Apache < 2.2.9 Multiple Vulnerabilities (DoS, XSS)*	1.0	0.61	0.74	0.0	0.275	0.0	2.9	8.6	4.3	*Medium*
16	*SSL Medium Strength Cipher Suites Supported*	1.0	0.61	0.74	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
17	*Apache 2.2 < 2.2.18 APR apr_fnmatch DoS*	1.0	0.61	0.74	0.0	0.0	0.275	2.9	8.6	4.3	*Medium*
18	*Apache 2.2 < 2.2.21 mod_proxy_ajp DoS*	1.0	0.61	0.74	0.0	0.0	0.275	2.9	8.6	4.3	*Medium*

Tabel 21. Lanjutan *Business Impact Analysis* Server Eproc

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
19	*Apache HTTP Server httpOnly Cookie Information Disclosure*	1.0	0.61	0.74	0.275	0.0	0.0	2.9	8.6	4.3	Medium
20	*SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection*	1.0	0.35	0.74	0.0	0.275	0.0	2.9	4.6	2.6	Low
21	*SSL / TLS Renegotiation DoS*	1.0	0.35	0.74	0.0	0.0	0.275	2.9	4.6	2.6	Low

Tabel 22. *Business Impact Analysis* Server SIPKD

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
1	*35362 MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
2	*Conficker Worm Detection (uncredentialed check)*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
3	*MS09-039: Vulnerabilities in WINS Could Allow Remote Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
4	*HP* Sistem *Management Homepage < 6.3 Multiple Vulnerabilities*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
5	*Multiple Vendor DNS Query ID Field Prediction Cache Poisoning*	1.0	0.71	0.74	0.0	0.660	0.660	9.2	10	9.4	*High*
6	*MS11-035: Vulnerability in WINS Could Allow Remote Code Execution*	1.0	0.61	0.74	0.660	0.660	0.660	10	8.6	9.3	*High*
7	*MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution*	1.0	0.61	0.74	0.660	0.660	0.660	10	8.6	9.3	*High*
8	*HP* Sistem *Management Homepage < 6.2 Multiple Vulnerabilities*	1.0	0.71	0.56	0.660	0.660	0.660	10	8	9	*High*
9	*JBoss JMX Console Unrestricted Access*	1.0	0.71	0.704	0.275	0.275	0.275	6.4	10	7.5	*High*
10	*SSL Certificate Cannot Be Trusted*	1.0	0.71	0.704	0.275	0.275	0.0	4.9	10	6.4	*Medium*
11	*SSL Self-Signed Certificate*	1.0	0.71	0.704	0.275	0.275	0.0	4.9	10	6.4	*Medium*
12	*Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness*	1.0	0.35	0.704	0.275	0.275	0.275	6.4	4.9	5.1	*Medium*

Tabel 23. Lanjutan *Business Impact Analysis* Server SIPKD

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
13	*Chargen UDP Service Remote DoS*	1.0	0.71	0.704	0.0	0.0	0.275	2.9	10	5	*Medium*
14	*Multiple Server Crafted Request WEB-INF Directory Information Disclosure*	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*
15	*DNS Server Cache Snooping Remote Information Disclosure*	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*
16	*SSL Certificate Expiry*	1.0	0.71	0.704	0.0	0.275	0.0	2.9	10	5	*Medium*
17	*Microsoft Windows SMB NULL Session Authentication*	1.0	0.71	0.704	0.275	0.0	0.0	2.9	10	5	*Medium*
18	*SMB Signing Disabled*	1.0	0.71	0.704	0.0	0.275	0.0	2.9	10	5	*Medium*
19	*SSL Weak Cipher Suites Supported*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
20	*SSL Medium Strength Cipher Suites Supported*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
21	*Terminal Services Encryption Level is Medium or Low*	1.0	0.61	0.704	0.275	0.0	0.0	2.9	8.6	4.3	*Medium*
22	*SSL Certificate Signed using Weak Hashing Algorithm*	1.0	0.35	0.704	0.275	0.275	0.0	4.9	4.9	4	*Medium*
23	*Terminal Services Encryption Level is not FIPS-140 Compliant*	1.0	0.35	0.704	0.275	0.0	0.0	2.9	4.9	2.6	*Low*
24	*SSL / TLS Renegotiation DoS*	1.0	0.35	0.704	0.0	0.0	0.275	2.9	4.9	2.6	*Low*

Tabel 24. *Business Impact Analysis* Server Simpeg

NO	*VULNERABILITY*	AV	AC	Au	C	I	A	IS	ES	*SCORE*	*LEVEL*
1	*MS03-026: Microsoft RPC Interface Buffer Overrun*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
2	*MS03-039: Microsoft RPC Interface Buffer Overrun*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
3	*MS04-007: ASN.1 Vulnerability Could Allow Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
4	*MS04-011: Security Update for Microsoft Windows*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
5	*MS05-027: Vulnerability in SMB Could Allow Remote Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
6	*MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*

7	*MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
8	*MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution*	1.0	0.71	0.74	0.660	0.660	0.660	10	10	10	*Critical*
9	*MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution*	1.0	0.71	0.74	0.275	0.275	0.275	6.4	10	7.5	*High*
10	*Microsoft Windows SMB NULL Session Authentication*	1.0	0.71	0.74	0.275	0.0	0.0	2.9	10	5	*Medium*
11	*SMB Signing Disabled*	1.0	0.71	0.74	0.0	0.275	0.0	2.9	10	5	*Medium*

3.3. Analisi *Business Impact Analysis* Jaringan Komputer dengan Menggunakan *Network Security assessment* pada Jaringan Pemerintah Kota Denpasar.

Hasil analisa dari *Network Security Assessment*pada jaringan Komputer Pemerintah Kota Denpasar mendapatkan *vulnerability* yang dimiliki oleh sistem. Jumlah *vulnerability* dapat dilihat pada tabel 25

Tabel 25. Jumlah *Vulnerability*

NO	NAMA SERVER	JUMLAH *VULNERABILITY*
1	Jempiring	5
2	Lawar	13
3	Email	20
4	Eproc	21
5	SIPKD	25
6	Simpeg	11

Server jempiring memiliki *vulnerability* sebanyak 5 buah, server lawar memiliki *vulnerability* sebanyak 13, server *email* memiliki *vulnerability* sebanyak 20, server eproc memiliki *vulnerability* sebanyak 21, server SIPKD memiliki *vulnerability* sebanyak 25, dan server simpeg memiliki *vulnerability* sebanyak 11.

Proses *Network Security Assessment* dilanjutkan ke tahap perhitungan *Business Impact Analysis* berdasarkan hasil *vulnerability* yang ditemukan di jaringan Pemerintah Kota Denpasar.Analisa dari perhitungan *Business Impact Analysis* tersebut didapatkan hasilkan tingkat resiko yang ditunjukkan pada tabel26.

Tabel 26. Hasil *Business Impact Analysis*

NO	NAMA SERVER	*LEVEL* RESIKO			
		Critical	*High*	*Medium*	*Low*
1	Jempiring	-	-	4	1
2	Lawar	-	-	10	3
3	Email	-	4	12	4
4	Eproc	2	3	14	2
5	SIPKD	5	5	13	2
6	Simpeg	8	1	2	-

4. Kesimpulan

Hasil dari proses Business Impact Analysis didapatkan kesimpulan sebagai berikut :

a. Hasil Network Security Assessmentmenunjukkan setiap server memiliki vulnerability, dengan rata rata vulnerability dari seluruh server sebanyak 15, 8 vulnerability.
b. Dari 6 server yang dilakukan Business impact analysis terdapat 4 server memiliki peringkat resiko critical atau high, yaitu server Email, Eproc, SIPKD, dan Simpeg.
b. Dalam melakukan penilaian Business Impact analysis disarankan untuk penelitian selanjutnya perhitungan kuantitatif digunakan dalam proses penilaian resiko.
c. Hasil dari Business Impact Analysis ini dapat dijadikan acuan untuk membangun disaster recovery planning

Daftar Pustaka:

[1] Hanif Al-Fatta. “Analisis & Perancangan Sistem Informasi untuk Keunggulan Bersaing Perusahaan & Organisasi Modern”. Andi Offset, Yogyakarta, 2007.
[2] Adi Nugroho. “Perancangan dan Implementasi Sistem Basis Data”. Andi Offset, Yogyakarta, 2011.
[3] Munawar. “Pemodelan Visual Dengan UML”. Yogyakarta. 2005.
[4] Prabowo Pudjo Widodo. “Menggunakan UML”. Informatika, Bandung, 2011.
[5] Prabowo Pudjo Widodo. “Menggunakan UML”. Informatika, Bandung, 2011.
[6] Kroll. P, Phillipe Kruchten. “The Rational Unified Process Made Easy:A Practitioner’s Guide to the RUP. Pearson Education”. Boston, MA. 2003.
[7] Abdul Kadir. “Dasar Pemrograan Web Dinamis Menggunakan PHP”, 2008, Andi Offset.
[8] Budi Raharjo, Imam Heryanto, Enjang RK. “Modul Pemrograman Web”. Modula, Bandung, 2010.
[9] Oleh Sholeh. “SQL sebagai Konsep Pembuatan Sistem Database”, 2006, Jurnal Cyber.